

Port Wars

*In the not-too-distant-future, firewalls spark a battle
over port regulation and ownership.*

By William Paul Fiefer

As operating system evolved, a large market emerged in add-ons. Little programs such as word processors, defragmenters, image viewers, and so forth appeared. You bought the OS, then you needed to keep on buying.

When the firewall becomes a killer application, it will need add-ons, too. In particular, it needs:

-- *Traffic analyzers* to deliver corporate intelligence reports and knowledge management (hard skill: stream parsing for corporate intelligence);

-- *Log enhancers*, so it can record a wide and adjustable (variable width and content type) swath of network traffic (hard skill: flexible, organic data structuring);

-- *Protocol port retainers* to reserve and protect for custom use specific Internet ports. The architecture of TCP/IP leaves a 16-bit field to count ports, meaning there can be only 65,536 of them and they are strategic turf (hard skill: socket programming and war hacking).

Only the most modular firewall designs will survive because modularity makes them easily extensible, a necessity in the new environment. This is so because new services often need new ports (or squabble over existing ports) and the firewall must take this into account. Firewalls today are not modular and are hard to add pieces to. Like any monolithic design, pack on too much and it turns brittle, snapping. A firewall that cannot be updated to flexibly and rapidly reserve, protect, monitor, analyze and release those valuable ports will be worthless.

The entities controlling and tweaking the master firewalls nearest the backbone are the governments, regulatory agencies, telcos, cable providers and satellite bandwidth suppliers. They have the undisputed port bottlenecking power. They are censors

delivering rivers of filtered information from the delta to segregated, internal communities.

Users further downstream will further screen the data with their own firewalls that other, sometimes smaller, service firms install and tweak. At the capillary nodes are parents and department bosses looking to protect their flock from the words "breast" and "thigh" and "job offer." Crackers will move in the trenches, attempt to hijack ports and place bugs, remote-control devices and banner ads for competitors on them.

As media and entertainment firms and big consulting shops jump into the act, this data sanitizing bottlenecking and port combat will be passed off as content programming and rough-and-tumble business. The "NYTimesNetNewsProtocol" and the "AllNudeNewsProtocol" will battle for port use under the leadership of pointy-haired blowhards from Accenture and PricewaterhouseCoopers. Wealthy entities, then, will ask the telcos and cable providers et al. to tweak their firewalls; wealthier entities will contract to multiple firewall providers (using at least one for data security and the rest for the custom content only Disney and Time-Warner and the local house of worship can provide).

Small fry and home users will be on their own and they will see sticker shock. The existing home-alarm and consumer-security firms will take to this market and consultants will move in to train and supply their staff. Eventually the home-alarm and consumer-security firms will consolidate into fewer, larger enterprises.

The porn industry will supply the amusement factor here, providing encrypted, fetish-tuned streams to dedicated IP ports within virtual communities of like-minded affectionate souls. You will turn on the news to learn of the newest court-battle over who is allowed to communicate using specific ports, whether a port can be privately owned, and whether these are Constitutional rights. Welcome to tomorrow.

William Paul Fiefer (yamada@prairienet.org) edits Web sites in the Chicago region. You can visit him at <http://www.prairienet.org/~yamada>.

Source: Ubiquity, Volume 4, Issue 35, Oct. 29 - Nov. 4, 2003